

FILED

Oct 21 - 2021

John M. Domurad, Clerk

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Northern District of New York

UNITED STATES OF AMERICA)

v.)

Jason S. Miller)

Case No. 8:21-MJ-502 (GLF)

Defendant(s))

CRIMINAL COMPLAINT


I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 25, 2020 in the county of Clinton in the Northern District of New York the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
Title 18, United States Code, Section 2252A(a)(2)(A)	Distribution of Child Pornography

This criminal complaint is based on these facts:
See attached affidavit

☒ Continued on the attached sheet.


Complainant's signature
Special Agent W. Jason Amoriell, FBI
Printed name and title

Attested to by the affiant in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Date: Oct. 21, 2021


Judge's signature

City and State: Plattsburgh, NY

Hon. Gary L. Favro, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

JASON S. MILLER,

Defendant.

Case No. 8:21-MJ-502 (GLF)

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, W. Jason Amoriell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a United States Federal Bureau of Investigation (FBI) special agent since completion of my training at the FBI Academy in June 2000. I am currently assigned to the Plattsburgh Resident Agency. In Plattsburgh and at my previous assignment at the Cedar Rapids Resident Agency, I have investigated criminal matters to include child pornography, wire fraud, and inter-state threats which involved social media, computers, and cellular telephones. Currently, my investigations include violations of 18 U.S.C. §§ 2251(a) and 2252A pertaining to the illegal production, distribution, receipt and possession of child pornography. I have received training in the area of child sexual exploitation and have observed and reviewed numerous examples of child pornography that has been stored or transmitted electronically. Since joining the FBI, I have interviewed victims and witnesses, and conducted searches of physical locations, social media, and electronic devices pursuant to court order or consent.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.
3. I make this affidavit in support of a criminal complaint charging the defendant, Jason S. Miller, with distributing child pornography, in violation of Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1).
4. The facts in this affidavit come from my training and experience, and information obtained from other agents, officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

5. On January 29, 2021, the FBI's Milwaukee Division sent the Albany Division information learned in a joint investigation with the Winnebago County Sheriff's Office (WCSO) that began in May 2020. The investigation concerns numerous groups engaged in the receipt, possession, distribution, and possible production of child pornography over the messaging application Kik Messenger ("KIK").
6. From my review of publicly available information provided by KIK about its service, including KIK's Law Enforcement Guide, KIK is a free smartphone messenger application that lets users send text, pictures and videos to other KIK users, and share sketches, mobile web-pages, linked internet files and other content.

7. To use the KIK application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and videos. During the registration process, KIK registers date, time, internet protocol (IP) address and device related information.
8. The username is the main unique identifier used by KIK. The second is the userid, which is the username with a short alpha-numeric addition after an underscore and is used within the KIK system. According to the KIK Law Enforcement Guide, a KIK username is unique, can never be replicated, and can never be changed.
9. KIK users are also able to create chat groups of up to 50 people to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, KIK users can share a link to the group with any other KIK user.
10. KIK permits users to create group hashtags. The hashtag is user generated, cannot be replicated, and cannot be changed. Like a username, it may include lower and uppercase letters, numbers, or period and underscores. It cannot contain spaces, emoticons or special characters.
11. An undercover investigator with the WCSO gained admission to a private group within KIK whose members were openly engaging in the distribution of child pornography.

The private group's name was "lilgurlhaven." The user deeplong9 was a member of "lilgurlhaven." Over the course of time spent within this group, multiple images and videos of child pornography were shared by its members. The user deeplong9 shared a video that was received by the undercover investigator. The undercover investigator provided this description: "Video depicts a pre-pubescent female approximately 5 to 8 years old with her vagina exposed. The prepubescent female then masturbates on camera. This video was sent on 05/25/2020 at approximately 11:10 pm CST. I did not have any private message conversations with this user." A copy of this video was provided to your affiant by FBI Milwaukee for initiating this investigation. I reviewed it, and the video is accurately described by the undercover investigator.

12. The Milwaukee Division served a subpoena on KIK c/o MediaLab.ai for basic subscriber information pertaining to KIK user "deeplong9." On August 12, 2020, KIK responded to the subpoena and advised that the first name associated with the account was "stressed", the last name associated with the account was "hello", and the unconfirmed e-mail address was stressedhello@hotmail.com. KIK also provided the IP address history that it still retained. The IP address history was used by the Milwaukee Division to serve a subpoena on an associated internet service provider, Charter Communications, Inc. ("Charter"), for two prevalently used IP addresses from the history. For the dates and times provided to Charter, an associated customer was identified as S.B. at a residence address in Plattsburgh, NY 12901. A second associated customer was V.M. at a residence address in Morrisonville, NY 12962.

13. The Milwaukee Division served a subpoena upon Microsoft, Inc. concerning the

Microsoft email stressedhello@hotmail.com. Microsoft, Inc. advised that stressedhello@hotmail.com was not a valid email address.

14. The Milwaukee Division served a subpoena upon Verizon Wireless for the Verizon Wireless associated IP addresses and date-time stamps from the KIK history. The Microsoft records identified phone number (XXX) XXX-6232 as the phone associated with the IP address use. This is a Tracfone mobile phone.
15. Tracfone records for (XXX) XXX-6232 contained no legitimate identifiers for the phone subscriber's identity. Associated social media accounts also contained no legitimate identifiers for the account user. Similarly, the user picture for the KIK account with the username deeplong9 contained no photograph clearly portraying the owner of the account. The user picture is an individual at a distance standing on a jetty in a large lake that resembles Lake Champlain overlaid on a photograph of a cliff with a mountain in the back that resembles the High Peaks region. I believe the use of the anonymized mobile phone and social media accounts are indicators that these are used for the purpose of collecting and distributing child pornography. The Tracfone records also indicated the phone's electronic serial number was 357092102453293, was purchased from Wal Mart store 5360, and was activated on June 11, 2019 with a service end date of June 13, 2020.
16. On February 22, 2021, I reviewed the Charter subpoena return that I was provided by Milwaukee Division along with the other investigative materials they developed for the opening of my investigation. The Charter return provided subscriber information for two Charter internet protocol (IP) addresses used for accessing the KIK account,

68.191.9.152 and 68.113.161.102 as previously mentioned in paragraph 12. These IP addresses were contained in the KIK records provided by KIK to the Milwaukee Division in its historical records for username deeplong9 spanning a usage period between May 26, 2020 and June 25, 2020. These KIK records also indicated that the user's device was a Samsung SM-S767VL.

17. Charter's IP address 68.191.9.152 was assigned to S.B. at a residence address in Plattsburgh, NY 12901. Charter's IP address 68.113.161.102 was assigned to V.M. at a residence address in Morrisonville, NY. The KIK records contained 517 connections for the IP address assigned to S.B. and occurred on a daily basis from June 8, 2020 through June 25, 2020 (the last day of the records) except on June 20, 2020. The KIK records for the IP address assigned to V.M. were only on June 13, June 14, June 20, and June 21, 2020, suggesting this was not the user's primary address, and the user's primary address was associated with S.B.

18. The KIK IP history also contained entries for the IP address 216.27.113.23 starting on June 3, 2020 and continuing through June 25, 2020. This IP address belongs to internet service provider Firstlight Fiber. On March 3, 2021, Firstlight Fiber provided me the user to whom this IP address is assigned pursuant to a subpoena. This IP address is assigned to the company B3CG USA at 18 Northern Avenue #7A, Plattsburgh, NY 12903 with a billing contact of K.S., the HR manager.

19. On March 4, 2021, I interviewed K.S. K.S. advised that V.M. is an employee at B3CG USA. His cell phone number was (XXX) XXX-0404. (The Verizon records for (XXX) XXX-6232 provided to me by the Milwaukee Division showed multiple texts between

these two numbers.) K.S. did not have the phone number (XXX) XXX-6232 in her employee database. She advised that V.M.'s friend, Jason Miller, had also worked at B3CG until his termination on October 30, 2020 due to being in jail. K.S. advised that B3CG did not have a phone number for Miller, because he never had a stable phone number. Miller and V.M. did not have work computers, but they were able to access B3CG's WI-Fi system via their phones. K.S. also reviewed the KIK connection times associated with the B3CG IP address and advised that those times all corresponded to Jason Miller's first break, dinner half hour, or final break.

20. On March 5, 2021, I interviewed Probation Officer Nicole Poupore, the former probation officer for Jason Miller. Officer Poupore advised that Miller's probation was revoked in October 2020 due to violating the terms of his probation for use of alcohol, pornography, and social media. While under her supervision, Miller's cell phone number was (XXX) XXX-6232. His activities included hiking, which is consistent with the KIK user picture described in paragraph 15. Officer Poupore confirmed that Miller has a friend named V. By June 2020, Miller was living with S.B. in Plattsburgh. Prior to living with S.B., Miller lived at America's Best Value Inn.

21. On March 5, 2021, Investigator John Whalen of Clinton County Department of Social Services advised that Jason Miller applied for benefits on July 30, 2018. In this application, Miller provided an address of 73 Margaret Street in Plattsburgh and a phone number of (XXX) XXX-6232.

22. On March 10, 2021, I interviewed S.B. S.B. advised that she lived at a Plattsburgh address in approximately December 2019 or January 20. After that, she moved to

another address in Plattsburgh. Jason Miller moved in with her in May or June 2020 and paid rent to her. S.B. has had password protected WI-FI in her residence since the start and provided its password to Miller for playing his X-Box. S.B. never saw Miller with a computer. S.B. assumed Miller also used the WI-FI access for his cell phone because he was always using it. Miller's phone was a Samsung Galaxy with telephone number (XXX) XXX-6232, which is stored in her phone. S.B. does not own a KIK account. Miller told her that he had a KIK account and Meet Me account.

23. S.B. advised that she never distributed or saw any child pornography at her home. Miller would pull his phone in close so that she could not view its screen sometimes when she walked by him. Miller's friends, A and V, got all of his property from S.B.'s residence approximately two weeks after his arrest for violation of his probation. Miller talked to a 17-year-old girl on his Meet Me account. Miller informed S.B. that the girl was of age, but a common acquaintance informed S.B. that the girl was 17 years old.

24. On March 17, 2021, I interviewed A.U. of the Morrisonville, NY address provided by Charter and described above in paragraph 17. A.U. advised that she knew Jason Miller from her previous employment at B3CG, where they both worked. A.U. started at B3CG in May 2018, and Miller was already employed there. Jason Miller's phone number has been (XXX) XXX-6232 since she has known him.

25. A.U. moved to her current residence in October 2019, and Miller visited her and V.M., who also lives there, at their residence. They have had password protected WI-FI at their residence the entire time, and A.U. believed they probably gave Miller access to their network. A.U. has never heard of KIK and does not know of anyone who has used

her network to access child pornography. A.U. and V.M. picked up his items from S.B. after his arrest. She found Miller's phone in the box of his items and has not deleted anything from his phone. She has used his phone to do his taxes and review the pictures stored on his phone. She saw no child pornography pictures. She did not review the videos stored on Miller's phone. Miller calls her nearly daily from prison and advised that she was probably the only one with the password to his phone. By checking her calendar for a birthday party with which Miller assisted, A.U. determined that Miller was at her home on June 19, 2020 and June 20, 2020. A.U. could not determine the additional days that Miller had visited.

26. A.U. provided me with Miller's phone. I used the Samsung phone's "About phone" page for the phone's serial number, which I used for the property receipt that I provided to A.U. for the phone. The phone's serial number is not visible on the phone's exterior. According to its "About phone" screen, its phone number is (XXX) XXX-6232, its model number is SM-S767VL and its IMEI is 357092102453293, which matches the Tracfone record in paragraph 15 and Kik record in paragraph 16.

27. After interviewing A.U., I interviewed V.M. V.M. also had the phone number for Jason Miller stored in his cell phone, (XXX) XXX-0404. According to V.M.'s entry, Miller's cell phone number is (XXX) XXX-6232. V.M. has known Miller for approximately four years and believes Miller has used that phone number the entire time.

28. V.M. did not own a KIK account and was not aware of Miller having a KIK account. V.M. never accessed KIK from his internet network. V.M. was sure that Miller had the home's WI-FI password, because it is located on the back of the router. Miller never


discussed child pornography with V.M. The images that they shared via text were of the games that they both played on X-Box. V.M. had no knowledge of Miller viewing or possessing child pornography and advised that Miller did not confide in him about his personal life.

29. On April 13, 2021, a search warrant was issued for Jason Miller's Samsung SM-S767VL cell phone. New York State Police's Computer Crime Unit examined this cell phone pursuant to the warrant and produced a report, which I have reviewed. Texts contained on the phone appear to be between V.M. and Jason Miller concerning his October 2020 hearing for the violation of his probation conditions that are described above in paragraph 20. Additionally, there is a text from (216) 327-6099 concerning erectile dysfunction addressed to a recipient named Jason. Furthermore, there is a text from the CVS Loyalty program addressed to a recipient named Jason concerning the reward program and a text from Verizon addressed to a recipient named Jason concerning a promotion.

30. The phone did not contain the video that was distributed and described above in paragraph 11; however, it did contain ten thumbnail image files that appear to be child pornography. The original full-size image files were no longer still on Miller's phone. These images were sent to the National Center for Missing and Exploited Children (NCMEC) for analysis. On August 19, 2021, NCMEC reviewed the images and determined that two images belonged to two series of known child pornography images. Investigator David Hungerford of New York State Police, who performed the extraction of Miller's cell phone, advised that in his investigative experience child pornography

images are frequently used by the possessors for sexual gratification and then deleted to preclude someone from discovering the images on the device. The phone also contained thumbnails of selfies that appear to be Jason Miller. Thumbnail images of two selfies appear to be Miller standing naked in front of a mirror with his cell phone. Additionally, there appear to be several thumbnail images of Miller's penis.

31. As stated above, there is probable cause to believe that the defendant distributed child pornography in violation of Title 18, United States Code, Section 2252A(a)(2)(A).


W. Jason Amoriell
Special Agent, FBI

I, the Honorable Gary L. Favro, United States Magistrate Judge, hereby acknowledge that this affidavit was attested to by the affiant by telephone on October 21, 2021 in accordance with Rule 41 of the Federal Rules of Criminal Procedure.

4:05 PM


Hon. Gary L. Favro
United States Magistrate Judge